IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

In re Application of:	Veijo VANTTINEN *et al.*	Confirmation No.:	9980
Application No.:	09/864,017	Examiner:	Truong, Thanhnga B.
Filed:	May 23, 2001	Group Art Unit:	2438

For: METHOD FOR PROCESSING LOCATION INFORMATION RELATING TO A TERMINAL CONNECTED TO A PACKET NETWORK VIA A CELLULAR NETWORK

Commissioner for Patents
Alexandria, VA 22313-1450

APPEAL BRIEF

Dear Sir:

This Appeal Brief is submitted in support of the Notice of Appeal dated January 31, 2011.

I. REAL PARTY IN INTEREST

The real party in interest is Nokia Corporation.

II. RELATED APPEALS AND INTERFERENCES

Appellants are unaware of any related appeals and interferences.

III. STATUS OF THE CLAIMS

Claims 1-32, 35 and 36 are pending in this Application, in which claims 33 and 34 have been canceled. Claims 2, 4, 6, 8, and 18-20 are original claims, and claims 1, 3, 5, 7, 9-17, 21-32, 35, and 36 have been previously presented.

Claims 27, 28, 31, and 32 were finally rejected in an Office Action dated October 29, 2010 and claims 29 and 30 were objected to in the October 29, 2010 Office Action as being dependent upon a rejected base claim, but would be allowable if recast in independent form. Claims 1-26, 35 and 36 stand allowed. It is from the final rejection of claims 27, 28, 31, and 32 on October 29, 2010, that this Appeal is taken.

IV. STATUS OF AMENDMENTS

No Amendment has been filed subsequent to the issuance of the Final Office Action on October 29, 2010.

V. SUMMARY OF THE CLAIMED SUBJECT MATTER

The claimed invention addresses problems associated with processing location information relating to a terminal connected to a packet network via a cellular network. The claimed invention is directed to an apparatus for receiving, from a mobile station, information relating to a location information request and a sender of the location information request, and determining to exchange information about a security association with a network element connected to a cellular network, the security association pointing to the network element from the sender of the location information request.

Independent claim 27 reads as follows:

27. An apparatus comprising:

at least one processor (See e.g., Specification FIG. 9, page 17, line 8 – page 18, line 34); and

at least one memory including computer program code (See e.g., page 17, line 8 – page 18, line 34), the at least one memory and the computer program code being configured, with the at least one processor, to cause the apparatus at least to:

receive, from a mobile station, information relating to a location information request and a sender of the location information request (See e.g., Specification FIG. 9, page 17, line 8 – page 18, line 34) and

determine to exchange information about a security association with a network element connected to a cellular network, the security association pointing to the network element from the sender of the location information request (See e.g., Specification FIG. 9, page 17, line 8 – page 18, line 34).

28. An apparatus according to claim 27, wherein the apparatus is at least further caused to:

determine to establish a second security association, which points to the apparatus from the sender of the location information request and at least specifies data origin authentication (See e.g., Specification FIG. 9, page 17, line 8 – page 18, line 34).

VI. GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

A. Claims 27 and 28 were rejected under 35 U.S.C. § 103(a) for obviousness predicated upon *Linden et al.* (US 6,549,773) in view of *Dent et al.* (US 5,812,955).

B. Claims 31 and 32 were rejected under 35 U.S.C. §103(a) for obviousness predicated upon *Linden et al.* in view of *Dent et al.*, and further in view of *Wang et al.* (US 6,415,773).

VII. ARGUMENT

A. CLAIMS 27 AND 28 ARE NOT RENDERED OBVIOUS BY *LINDEN ET AL.* AND *DENT ET AL.* BECAUSE *LINDEN ET AL.* AND *DENT ET AL.*

FAIL TO DISCLOSE OR RENDER OBVIOUS ALL OF THE RECITED FEATURES OF THESE CLAIMS.

The Examiner bears the initial burden of establishing a *prima facie* basis to deny patentability to a claimed invention under any statutory provision. In rejecting a claim under 35 U.S.C. §103(a), the Examiner is required to provide a factual basis to support the obviousness conclusion. *In re Warner*, 379 F.2d 1011, 154 USPQ 173 (CCPA 1967); *In re Lunsford*, 357 F.2d 385, 148 USPQ 721 (CCPA 1966); *In re Freed*, 425 F.2d 785, 165 USPQ 570 (CCPA 1970). Further, in rejecting a claim under 35 U.S.C. §103(a) it is incumbent upon the Examiner to establish the requisite motivation. As maintained by the Supreme Court of the United States in *KSR Intern. Co. v. Teleflex Inc.*, 127 S.Ct. 1727 at 1741, an obviousness "analysis should be made explicit." See, *In re Kahn*, 441 F.3d 977, 988 (C.A. Fed. 2006) ("[R]ejections on obviousness grounds cannot be sustained by mere conclusory statements; instead, there must be some articulated reasoning with some rational underpinning to support the legal conclusions of obviousness"). Indeed, the Examiner is required to make specific factual findings, not generalizations. *See M.P.E.P. §2144.08 II. A. 5.* That initial burden required by procedural due process of law has not been discharged.

Independent claim 27 recites, *inter alia*, "receive, from a **mobile station**, information relating to a location information request and a **sender of the location information request**" and "determine to exchange **information about a security association** with a **network element** connected to a cellular network, the security association **pointing to the network element from the sender of the location information request**."

The Final Office Action (on pages 2, 3, and 6) cites Figure 1 and col. 6, lines 57-66, col. 10, lines 6-8, and col. 11, lines 59-62 of *Linden el al.* and alleges that *Linden el al.* discloses the above discussed features. Appellants respectfully disagree.

Specifically, *Linden et al.*, in pertinent part, discloses (emphasis added):

Col. 6, Lines 1-15: Communication devices, i.e. wireless communication devices MS1 and MS2, advantageously **mobile stations (MS) function as clients 1 and are connected to a gateway 2, which is advantageously a server** and which adapts the different data transmission protocols used to each other. The clients 1 utilize advantageously a public land mobile network (PLMN), such as the GSM network and the GSM GPRS network, in order to implement wireless data transmission. The base station subsystem (BSS) of the mobile communication network (PLMN) is known as such and comprises base transceiver stations (BTS) and base station controllers (BSC). **The mobile station MS1, MS2 communicates with a base transceiver station via a radio channel**, and the base transceiver station communicates further with a base station controller.

Col 6, Lines 57-66: A smart card used in mobile phones is a so-called SIM card, which in modern mobile phones is typically a small-sized mini-card inserted in the telephone. The function of the card is, for instance, to store subscriber data and identifications (PIN, Personal Identification Number), and thus the card determines the subscriber number of the telephone. The SIM card can also contain a stored list of telephone numbers or a group of short messages, as well as various data and set values related to the communication network used.

Col. 10 Lines 6-8: The WSP layer provides means for **exchanging the information content between the applications of the client 1 and of the server 3**.

Col. 11, Lines 38-63: With reference to FIG. 6, at the next stage, the WDP layer 105 detects that the destination address belongs to a local mobile station MS, i.e. to the wireless communication device MS, to which the smart card SC is coupled as well, wherein the indication is transmitted (stage 204) to the appropriate port in the smart card interface 4. The smart card interface 4 processes the indication and processes the WSP/B request by making the necessary requests to the smart card SC (stage 205). After this, the smart card SC gives the content of the desired file to the smart card interface 4 (stage 206), after which the interface 4 encapsulates the content in the WSP/B response and transmits (stage 207) it as a request to the WDP layer 105. At the next stage 208, it is detected in the WSP layer 102 that the destination address and the destination port of the request belong to the browser 101 of the local mobile station MS, and the indication is transmitted (stage 208) to the WSP layer. After this, the WSP layer 102 transmits (stage 209) a WSP/B response to the browser 101, and the browser 101 presents the content of the file to the user (stage 210), advantageously by using the user interface 5. **The aforementioned WSP/B requests and responses can contain necessary header information, related, for example, to the content type of the message and to the authentication and authorization of the user**. Furthermore, they can include data relating to the compression method used and data for parity checking.

Linden et al. is generally directed to a method of data transmission between mobile stations and a server, and merely discloses means for exchanging information content between the applications of the client and the server (see *Linden et al.*, col. 10, lines 6 through 8). *Linden et al.* also discloses that a mobile phone can have a smart card that may store subscriber data and identifications (see *Linden et al.*, col. 6, lines 57 through 66). As best understood, the Final Office Action considers the subscriber data and identifications stored on the smart card of *Linden et al.* as corresponding to the claimed security association. However, it is clear from the above reproduced passages and Figure 1 of *Linden et al.*, that *Linden et al.* simply discloses that an information exchange takes place between a client 1 and a gateway 2 (a server) and that WSP/B requests and responses can contain header information to the content type of the message and to the authentication and authorization of the user, but makes no mentioning of a **location information request**. Moreover, *Linden et al*. does not disclose, nor suggest, an apparatus that receives, **from a mobile station**, information relating to a location information request and **a sender of the location information request**, and determines to exchange information about a security association with **a network element connected to a cellular network**, the security association **pointing to the network element from the sender of the location information request**. That is, *Linden el al*. fails to disclose that the subscriber data or identifications (the alleged security association) **points to** a network element connected to a cellular network **from** a sender of a location information request.

Thus, Appellants respectfully submit that the system of *Linden el al.* cannot reasonably be considered to disclose the above discussed features of independent claim 27. In addition, the secondary reference to *Dent et al.* does not cure the deficiencies of *Linden et al.* Thus, whether taken alone or in combination, and Appellants certainly do not agree that the requisite fact-based

motivation has been established for combining the applied references, the combination of *Linden et al.* and *Dent el al.* fails to teach or render obvious all of the recited features of independent claim 27. Therefore, independent claim 27 is patentable over the combination of *Linden et al.* and *Dent el al.*

In addition, dependent claim 28 is patentable, at least in view of the patentability of independent claim 27, from which this claim depends, as well as for the additional features this claim recites. For example, dependent claim 28 recites, *inter alia*, "determine to establish **a second security association**, **which points to the apparatus from the sender of the location information request and at least specifies data origin authentication**." Neither *Linden et al.* nor *Dent el al.* discloses or renders obvious the claimed second security association **that points to the apparatus from the sender of the location information request**.

Therefore, Appellants respectfully submit that the imposed rejection of independent claim 27, and dependent claim 28, under 35 U.S.C §103(a) for obviousness based on *Linden et al.* and *Dent el al.* is not factually or legally viable. Hence, the rejection of independent claim 27, and dependent claim 28, must be reversed, because *Linden et al.* and *Dent el al.* do not disclose or render obvious the features of these claims. Accordingly, reversal of this rejection by the Honorable Board is respectfully solicited.

B. CLAIMS 31 AND 32 ARE NOT RENDERED OBVIOUS BY *LINDEN ET AL.*, *DENT ET AL.*, AND *WANG ET AL.*, BECAUSE *LINDEN ET AL.*, *DENT ET AL.*, AND *WANG ET AL.* FAIL TO DISCLOSE OR RENDER OBVIOUS ALL OF THE RECITED FEATURES OF THESE CLAIMS.

As stated above, the Examiner bears the initial burden of establishing a *prima facie* basis to deny patentability to a claimed invention under any statutory provision.

With respect to the 35 U.S.C. § 103(a) rejection of dependent claims 31 and 32, *Wang et al.* fails to at least remedy the above discussed deficiencies of *Linden et al.* and *Dent el al.*

Therefore, claims 31 and 32 also are patentable over *Linden et al.* and *Dent el al.*, for at least the reasons independent claim 27 is patentable, from which these claims depend, as well as for the additional features these claims recite. Even if, *arguendo*, the applied references are combined as proposed by the Examiner, and Appellants do not agree that the requisite basis for the asserted motivation has been established, the features recited in dependent claims 31 and 32 would not result.

Thus, the imposed rejection of dependent claims 31 and 32 under 35 U.S.C §103(a) for obviousness based on *Linden et al.*, *Dent el al.*, and *Wang et al.*, is not factually or legally viable. Hence, the rejection of claims dependent claims 31 and 32 must be reversed, because *Linden et al.*, *Dent el al.*, and *Wang et al.* do not disclose or render obvious all of the features of these claims. Accordingly, reversal of this rejection by the Honorable Board is respectfully solicited.

VIII. CONCLUSION AND PRAYER FOR RELIEF

Based on the foregoing, it is apparent that the Examiner's rejections under 35 U.S.C. § 103(a) are not factually or legally viable. Appellants therefore solicit the Honorable Board to reverse each of the Examiner's rejections.

To the extent necessary, a petition for an extension of time under 37 C.F.R. § 1.136 is hereby made. Please charge any shortage in fees due in connection with the filing of this paper, including extension of time fees, to Deposit Account 504213 and please credit any excess fees to such deposit account.

Respectfully Submitted,

DITTHAVONG MORI & STEINER, P.C.

March 31, 2011
Date

/Lenwood Faulcon, Jr./
Lenwood Faulcon, Jr.
Attorney/Agent for Applicant(s)
Reg. No. 61310

Phouphanomketh Ditthavong
Attorney for Applicant(s)
Reg. No. 44658

918 Prince Street
Alexandria, VA 22314
Tel. (703) 519-9951
Fax (703) 519-9958

IX. CLAIMS APPENDIX

1. A method comprising:

receiving a location information request at a first network element, which is connected to a cellular network, from a second network element, which is connected to a packet data network, the location information request relating to a mobile station associated with the cellular network;

determining to transmit a request to a third network element, which is connected to the packet data network, the request requesting a security document relating to the second network element;

determining to initiate establishment of at least one security association that at least specifies data origin authentication and points from the second network element to the first network element, wherein the establishment at least involves use of information comprised in the security document;

determining to authenticate, after successful establishment of the at least one security association, a data origin of the location information request; and

determining to initiate, if the data origin of the location information request is authenticated successfully, a location procedure relating to the mobile station.

2. A method according to claim 1, wherein the security document relating to the second network element is a public key certificate, which comprises an identifier specifying the second network element and a public key of the second network element and which is cryptographically signed by the third network element.

3. A method according to claim 1, further comprising:

determining to request, from the third network element, a second security document relating to the first network element.

4. A method according to claim 3, wherein the security document comprises a first key, which is encrypted using a second key shared between the first network element and the third network element, and the second security document comprises the first key, which is encrypted using a third key shared between the second network element and the third network element.

5. A method according to claim 3, further comprising:

determining to initiate establishment of a second security association that points from the first network element to the second network element using at least information comprised in the second security document.

6. A method according to claim 5, wherein the security association is a set of Internet Security Associations pointing from the second network element to the first network element and the second security association is a second set of Internet Security Associations pointing from the first network element to the second network element.

7. A method according to claim 5, wherein the second security association at least specifies data encryption.

8. A method according to claim 1, wherein the security association is a set of Internet Security Associations pointing from the second network element to the first network element.

9. A method according to claim 1, further comprising:

determining to generate the security document by the third network element, which is connected to the packet data network;

determining to initiate establishment of at least one other security association using at least information comprised in the security document, the at least one other security association at least specifying data origin authentication and pointing from the second network element to the first network element;

determining to authenticate, after successful establishment of the at least one other security association, a data origin of the location information request; and

determining to implement a location procedure, the location procedure relating to the mobile station.

10. A method according to claim 9, further comprising:

determining to transmit location information relating to the mobile station to the second network element.

11. A method according to claim 10, wherein the location information relating to the mobile station is determined to be transmitted to the second network element from the first network element.

12. A method according to claim 11, further comprising:

determining to generate a second security document by the third network element, the second security document relating to the first network element; and

determining to initiate establishment of a second security association using at least the information specified in the second security document, the second security association at least specifying data encryption and pointing from the first network element to the second network element.

13. A method according to claim 10, further comprising:

determining to initiate, before determining to transmit the location information to the second network element, establishment of a third security association, which at least specifies data origin authentication and points from the second network element to a packet data device, wherein the packet data device is either connected to the mobile station or is an integral part of the mobile station.

14. A method according to claim 10, wherein the location information relating to the mobile station is determined to be transmitted from a device, which is either connected to the mobile station or is an integral part of the mobile station.

15. A method according to claim 14, further comprising:

determining to initiate, before determining to transmit the location information to the second network element, establishment of a third security association, which at least specifies data origin authentication and points from the second network element to a packet data device, wherein the packet data device is either connected to the mobile station or an integral part of the mobile station.

16. A method according to claim 15, further comprising:

determining to initiate, before determining to transmit the location information, establishment of a fourth security association, which at least specifies data encryption and which points to the second network element from the packet data device.

17. A method according to claim 14, further comprising:

determining to receive via the mobile station a notification relating to the location procedure associated with the mobile station,

wherein the mobile station is configured to inform the packet data device about the notification.

18. A method according to claim 1, wherein the first network element is a network element of a GPRS network.

19. A method according to claim 18, wherein the first network element is a Gateway Mobile Location Center.

20. A method according to claim 1, wherein the first network element is a network element of a UMTS network.

21. An apparatus comprising:

at least one processor; and

at least one memory including computer program code, the at least one memory and the computer program code being configured, with the at least one processor, to cause the apparatus at least to:

receive, from a packet data network, a location information request relating to a mobile station,

determine to initiate a location procedure in a cellular network,

determine to initiate establishment of security associations pointing to the apparatus from a network element of a packet data network,

determine to perform security functions specified by the security associations on data received from the packet data network,

determine if there is an existing security association pointing to the apparatus from a sender of the location information request, and

determine to initiate security association establishments, which are configured to establish security associations if security associations do not exist, wherein the security association establishments point to the apparatus from the sender of the location information request.

22. An apparatus according to claim 21, wherein the apparatus is at least further caused to:

receive, from a device reachable via the cellular network, a request about a particular security association, which points to the apparatus from a certain network element of the packet data network;

determine whether the particular security association exists; and

determine to transmit information about the particular security association to the device.

23. An apparatus according to claim 21, wherein the apparatus is at least further caused to:

receive a request to generate security documents relating to the device and to the sender of ~~a~~ the location information request; and

determining to generate a first security document associated with the device and a second security document associated with the location information request.

24. An apparatus according to claim 21, wherein the apparatus is a network element of a GPRS network.

25. An apparatus according to claim 24, wherein the apparatus is a Gateway Mobile Location Center.

26. An apparatus according to claim 21, wherein the apparatus is a network element of a UMTS network.

27. An apparatus comprising:

at least one processor; and

at least one memory including computer program code, the at least one memory and the computer program code being configured, with the at least one processor, to cause the apparatus at least to:

receive, from a mobile station, information relating to a location information request and a sender of the location information request, and

determine to exchange information about a security association with a network element connected to a cellular network, the security association pointing to the network element from the sender of the location information request.

28. An apparatus according to claim 27, wherein the apparatus is at least further caused to:

determine to establish a second security association, which points to the apparatus from the sender of the location information request and at least specifies data origin authentication.

29. An apparatus according to claim 28, wherein the apparatus is at least further caused to:

determine to request a network element of the cellular network to generate security documents relating to the apparatus and to the sender of the information request,

wherein the security documents are utilized to establish the second security association.

30. An apparatus according to claim 27, wherein the apparatus is at least further caused to:

determine to transmit, to the mobile station, a permission to transmit location information to the sender of the location information request,

wherein the permission is transmitted to the mobile station if the security association is established.

31. An apparatus according to claim 27, further comprising a receiver of a positioning system.

32. An apparatus according to claim 31, wherein the receiver is a Global Positioning System receiver.

33. (Canceled).

34. (Canceled).

35. An apparatus comprising:

at least one processor; and

at least one memory including computer program code, the at least one memory and the computer program code being configured, with the at least one processor, to cause the apparatus at least to:

receive a location information request at a first network element, which is connected to a cellular network, from a second network element, which is connected to a packet data network, the location information request relating to a mobile station associated with the cellular network;

determine to transmit a request to a third network element, which is connected to the packet data network, the request requesting a security document relating to the second network element;

determine to initiate establishment of at least one security association that at least specifies data origin authentication and points from the second network element to the first network element, wherein the establishment at least involves use of information comprised in the security document;

determine to authenticate, after successful establishment of the at least one security association, a data origin of the location information request; and

determine to initiate, if the data origin of the location information request is authenticated successfully, a location procedure relating to the mobile station.

36. An apparatus according to claim 35, wherein the apparatus is further caused to:

determine to generate the security document by the third network element, which is connected to the packet data network;

determine to initiate establishment of at least one other security association using at least information comprised in the security document, the at least one other security association at least specifying data origin authentication and pointing from the second network element to the first network element;

determine to authenticate, after successful establishment of the at least one other security association, a data origin of the location information request; and

determine to implement a location procedure, the location procedure relating to the mobile station.

X. EVIDENCE APPENDIX

Appellants are unaware of any evidence that is required to be submitted in the present Evidence Appendix.

XI. RELATED PROCEEDINGS APPENDIX

Appellants are unaware of any related proceedings that are required to be submitted in the present Related Proceedings Appendix.